Blockchain en smart contracts

Goossens, Jurgen; Verslype, Kristof

Published in:
Eerste hulp bij rechtszaken

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Blockchain en smart contracts: het einde van de vertrouwde tussenpersoon?[1]

Jurgen Goossens
Postdoctoraal onderzoeker UGent
Universitair docent staatsrecht Erasmus Universiteit Rotterdam

Kristof Verslype
Doctor in de ingenieurswetenschappen, onderzoeker, adviseur en spreker bij Smals
ICT-dienstverlener voor overheidsinstellingen

Blockchain is een revolutionaire technologie waar heel wat potentieel aan toegeschreven wordt. Het zou de rol van vertrouwde tussenpartijen zoals banken of notarissen doen verdwijnen of op zijn minst leiden tot een herdefiniëring van hun werking en taken. Ongetwijfeld zal deze technologie ook een grote impact hebben op de juridische sector.

1. Inleiding

Blockchain wordt beschouwd als een grondleggende technologie. Wat het Internet betekende voor het snel en goedkoop uitwisselen van informatie, belooft blockchain waar te maken voor het uitwisselen van waarde. Blockchain zou een ingrijpende impact kunnen hebben op verscheidene domeinen van de samenleving. Het zou nieuwe fundamenten kunnen leggen voor ons economisch en sociaal systeem. Hoewel de impact enorm zou kunnen zijn, zal het nog geruime tijd duren vooraleer blockchain tot zijn volle potentieel komt. In elk geval is er dringend nood aan advocaten, bedrijfsjuristen, gerechtsdeurwaarders, academici, beleidsmakers en rechters die hierover expertise opbouwen.

Er zijn weliswaar nog heel wat fundamentele technische en juridische vragen die vooralsnog onduidelijk of onbeantwoord zijn. Denk op juridisch vlak bijvoorbeeld aan de impact van de algemene verordening gegevensbescherming of de rechtsgevolgen en aansprakelijkheid bij een smart contract (zie onder). Het is daarnaast ook cruciaal om voor ogen te houden dat interactie tussen de technologie en juridische vraagstukken cruciaal is, bijvoorbeeld op het vlak van privacy. Blockchaintechnologie komt niet in een juridisch vacuüm terecht. Het functioneert binnen het bestaande wetgevende kader, waarbij de huidige stand van wetgeving en rechtspraak evenwel moeite heeft om de snelle technologische evoluties bij te benen.

[1] Deze bijdrage werd gepubliceerd in het online tijdschrift *Actua Leges*.

Het in 2009 gelanceerde Bitcoin is de eerste toepassing – en nog steeds een van de meest populaire – die onderliggend blockchaintechnologie gebruikt. Bitcoin laat toe om digitaal waarde (virtuele munten of cryptomunten) te creëren en te verhandelen zonder een intermediaire tussenpersoon, zoals een bank. Al vrij snel werd duidelijk dat de technologie gebruikt kan worden om ook in heel wat andere toepassingen en domeinen het optreden en de afhankelijkheid van intermediaire partijen omwille van de noodzaak aan vertrouwen te reduceren en zelfs volledig weg te nemen. Blockchain wordt dan ook gezien als een technologie voor disintermediatie. Allerlei handelingen die vandaag een tussenpartij vereisen, zouden dankzij blockchain ook zonder deze tussenpartij mogelijk worden. Blockchain, of de ruimere term *Distributed Ledger Technology* (DLT), beoogt dus de tussenkomst van *Trusted Third Parties* (TTP) overbodig te maken. Een blockchaintoekomst is dus een toekomst zonder intermediaire partijen of – in onze realistische visie – een toekomst met een beperktere taakstelling voor bijvoorbeeld notarissen, commerciële internetplatformen, beheerders, banken of overheden.

2. Wat is blockchain?

In essentie is blockchain een gegevensstructuur – een soort gegevensbank – waar enkel collectief door het peer-to-peer netwerk (zonder centrale partij) digitaal ondertekende gegevens aan toegevoegd kunnen worden. Het is wel nodig dat deze gegevens aan bepaalde voorwaarden (regels) voldoen, wat eveneens collectief geverifieerd wordt. Aan de Bitcoin-blockchain kunnen we bijvoorbeeld transactiegegevens toevoegen die, vereenvoudigd, een dergelijke boodschap bevatten: "Ik, Bob, wil een halve bitcoin transfereren naar Alice". Het netwerk verifieert collectief of de ondertekenaar van de transactie, Bob, over voldoende onuitgegeven bitcoins beschikt en, indien dit zo is, wordt de transactie door het netwerk aanvaard door ze aan de blockchain toe te voegen. De blockchain bevat dus de volledige historiek van alle transacties. Daaruit kan afgeleid worden hoeveel bitcoins iedereen bezit.

Die transacties worden gegroepeerd in blokken die met een bepaalde frequentie collectief door het netwerk achteraan de blockchain toegevoegd worden. 'Blockchain' is dus een keten (*chain*) van blokken. Bij Bitcoin is de streeffrequentie bijvoorbeeld één blok per tien minuten. Het laatste blok bevat bijgevolg de meest recent verwerkte transacties. De blockchain bevat dus alle verwerkte transacties, van de allereerste tot de allerlaatste. Vanaf de opname in de blockchain zijn de transacties in principe onwijzigbaar en niet verwijderbaar. Vele participanten in het blockchainnetwerk bezitten een lokale kopie van de blockchain die ze up-to-date houden. We noemen hen *nodes*. Iedereen heeft dus dezelfde versie van de blockchain. De technologie

kan hierdoor gebruikt worden voor het uitwisselen van gegevens en garandeert dat iedereen over dezelfde en meest actuele informatie beschikt. Elk blok bevat een tijdstempel die door het netwerk collectief gevalideerd is. We weten dus exact wanneer een transactie in de blockchain opgenomen werd. Antidatering wordt zo uitgesloten.

Blockchain maakt daarbij intensief gebruik van cryptografie. Dit is het gebruik van wiskundige principes om gegevens te beschermen. Eigenschappen zoals integriteit en confidentialiteit van gegevens kunnen met behulp van cryptografie gegarandeerd worden. Het gebruik van cryptografie impliceert natuurlijk niet automatisch dat alles ook 100% veilig is.

Er is een belangrijk verschil tussen *permissionless* en *permissioned* bockchainnetwerken. *Permissionless* bockchainnetwerken zijn netwerken waarin iedereen gelijke rechten heeft en zijn in de praktijk vaak publiek en open. Voorbeelden zijn Bitcoin, Ethereum en Litecoin. Vandaag gebruiken de voornaamste *permissionless* blockchainnetwerken Proof of Work (PoW) als consensusmechanisme, wat garandeert dat iedereen met dezelfde versie van de blockchain werkt. PoW heeft echter als nadeel dat het enorm veel energie verbruikt. *Permissioned* blockchainnetwerken zijn in de praktijk meestal afgeschermd. Rond het netwerk bevindt zich dan niet alleen een toegangscontrolelaag die bepaalt wie toegang heeft tot het blockchainnetwerk, maar ook vooral wie wat mag doen. zijn doorgaans. Zij zijn doorgaans een pak energie-efficiënter en sneller.

Hoewel de technologie als veelbelovend gezien wordt, zal het nog verschillende jaren duren vooraleer ze volwassen is. Dit impliceert dat het vandaag veel inspanning vergt, geld kost en ook risico's inhoudt om blockchaintoepassingen operationeel te maken en te houden. Toch houdt dit bedrijven en overheden niet tegen om reeds volop met de technologie te experimenteren. Daarbij worden veel *Proof of Concepts* (softwareprototypes) ontwikkeld, die weliswaar de mogelijkheden van de technologie illustreren, maar waar doorgaans verder niet veel meer mee gebeurt.

3. SMART CONTRACTS

Blockchain maakt meestal gebruik van smart contracts voor het collectief afdwingen van bepaalde regels. Een smart contract is een set van toepassingsspecifieke regels, uitgedrukt in computercode, die op een blockchain gepubliceerd worden en door het blockchainnetwerk collectief en correct uitgevoerd worden, waarbij het smart contract waarde kan ontvangen, blokkeren en transfereren. Dit laat toe om gedistribueerd, dus zonder centrale partij, afspraken tussen partijen af te dwingen. Een smart contract dwingt de toepassing af van de regel '*if this, than that*'. Indien dus aan bepaalde voor-

waarden wordt voldaan, vindt een bepaalde handeling of transactie plaats. Niemand kan daarbij de correcte uitvoering van het smart contract eenzijdig beïnvloeden. In toenemende mate zouden hierdoor, in theorie, geschillen en dus ook de nood aan een rechterlijke tussenkomst kunnen verdwijnen.

'Smart contract' is evenwel een misleidende benaming. Het is immers niet per se een 'contract' of een 'overeenkomst'. Het kan op zich het sluiten of het uitvoeren van een overeenkomst inhouden, maar dit hoeft niet. Zo kan het onder meer gaan over een verbintenis uit een eenzijdige wilsuiting, zoals bijvoorbeeld het ontslag van een werknemer, of een administratieve rechtshandeling (bv. een beschikking die voortvloeit uit een gebonden bevoegdheid). Het is daarnaast ook eerder deterministisch (*if x, than y*) dan 'smart'.

Een vastgoedtransactie enkel laten doorgaan nadat een geldig EPC en bodemattest afgeleverd zijn, en nadat de notaris aangegeven heeft dat de betrokkenen correct geïnformeerd zijn, is op een blockchain enkel te realiseren met behulp van smart contracts. De mogelijke toepassingen van blockchaingebaseerde smart contracts zijn bijzonder talrijk. Denk aan smart contracts voor veilingen, identiteitsbeheer, crowdfunding, huurwaarborg, smart locks, herkomst en toeleveringsketen, of verkiezingen.

4. (Nood aan) juridisch kader

Er zal telkens moeten worden nagegaan welke algemene en sectorspecifieke wet- en regelgeving in het betreffende rechtsdomein van toepassing is, afhankelijk van de sector waarin blockchain toegepast wordt. Dat heeft ook een impact op welke toezichthouders mogelijk een rol spelen, zowel op nationaal als op Europees vlak. In elk geval zal reeds in de ontwerpfase van de blockchain bij elke blockchaintoepassing telkens bijzonder veel aandacht moeten gaan naar de conformiteit met de privacywetgeving en dan vooral de Algemene Verordening Gegevensbescherming die op 25 mei 2018 in werking is getreden. Belangrijke principes van de AVG, zoals een behoorlijke en rechtmatige verwerking van persoonsgegevens, het recht op rectificatie en vergetelheid, het recht op beperking van de verwerking en passende beveiliging, stellen blockchainprojecten immers vaak voor grote uitdagingen. Gegevens die worden toegevoegd aan de blockchain, zijn immers niet wijzigbaar noch verwijderbaar, wat ook net tegelijkertijd de grootste troef is van blockchaintoepassingen. Hier is duidelijk sprake van een spanningsveld. In elk geval kan non-compliance met de AVG soms enkel vermeden worden door geen persoonsgegevens in de blockchain op te nemen, maar deze buiten de blockchain op te slaan of deze te anonimiseren vooraleer ze worden opgenomen. Dit kan dan wel weer een negatief effect hebben op de mogelijkheden van de blockchain.

België, noch de EU hebben reeds specifieke blockchainregelgeving aangenomen. Naast de bijzonder relevante analyse welke bestaande wet- en regelgeving mogelijks van toepassing zijn op blockchaintoepassingen en dus mogelijks een hinderpaal kunnen zijn bij de ontwikkeling van een concrete blockchain, zullen beleidsmakers, wetgevers en academici – in nauw overleg met technische specialisten – in de nabije toekomst ook moeten nadenken over nieuwe wetgevende kaders. Indien blockchain immers nog maar een gedeelte realiseert van wat het belooft, zal de impact ontegensprekelijk immens zijn. We hebben in dit opzicht nood aan doordachte wetgeving die toekomstbestendig is in een domein waar de snelheid van technologische evoluties enkel zal toenemen. Zo is blockchain slechts één mogelijke vorm, doch momenteel de meest populaire, van *Distributed Ledger Technology*. In de financiële sector en in de verzekeringssector zouden blockchain en smart contracts alvast aanzienlijke efficiëntiewinsten kunnen opleveren. De bestaande regelgeving in deze sectoren is echter vooral gericht op tussenpersonen, waardoor nieuwe gedecentraliseerde technologie zoals blockchain een nieuw regelgevend kader vereist.

Het principe van functionele equivalentie, zoals bijvoorbeeld ingebed in artikel 9.1 Richtlijn inzake elektronische handel, zou alvast als een goede inspiratiebron kunnen dienen bij nieuwe wetgevende initiatieven. Volgens de theorie van de functionele equivalentie moeten we ons niet blindstaren op het gekozen middel maar moeten we kijken naar de achterliggende doelstelling om te bepalen of aan wettelijke of reglementaire vormvereisten is voldaan. Ook bij blockchain of andere '*distributed ledger*'-technologieën zou dergelijke aanpak alvast voor meer rechtszekerheid kunnen zorgen. De wetgever kan het zich niet veroorloven om al te lang een juridisch vacuüm of onzekerheid inzake toepasselijke regelgeving in stand te houden. Dit staat immers op gespannen voet met het rechtszekerheidsbeginsel en kan in de praktijk een rem betekenen op nieuwe ontwikkelingen die de maatschappij ten goede zouden komen. Tenslotte moet ook worden gekeken naar het geschikte niveau om de juridische (en andere) uitdagingen inzake blockchain op te vangen. Elk land dient zich te bezinnen over regelgevend ingrijpen en het lijkt dat vooral de EU niet achter zal kunnen blijven om tot een geharmoniseerde aanpak te komen. Blockchaintoepassingen overschrijden immers al snel de landsgrenzen en blijven geregeld zelfs niet binnen het EU-grondgebied.

5. GEDISTRIBUEERD VERTROUWEN

Een blockchainnetwerk kan collectief ondersteuning bieden voor drie soorten acties die normaliter een vertrouwde partij vereisen: het registreren van feiten, het transfereren van activa en het afdwingen van regels. In de praktijk

is er vaak sprake van een combinatie. Gedistribueerd vertrouwen betekent trouwens niet dat de noodzaak aan vertrouwen verdwijnt. We moeten er nog steeds op vertrouwen dat een meerderheid eerlijk is, dat er zich geen veiligheidskwetsbaarheden of bugs in de blockchainsoftware van de participanten of in het smart contract bevinden, dat het smart contract doet wat de makers beloven, dat de cryptografische assumpties waar alles op steunt correct zijn en blijven, dat we onze private sleutel niet verliezen, dat het bedrijf dat onze virtuele munten beheert niet gehackt wordt, dat het netwerk niet gesatureerd is wanneer we het willen gebruiken etc. Indien extern aangeleverde gegevens in de blockchain geregistreerd worden, kan het blockchainnetwerk bovendien niet de correctheid van deze gegevens verifiëren (i.e. '*crap in, crap out*').

Er is tenslotte sprake van een blockchaintrilemma, namelijk een spanningsveld tussen veiligheid, schaalbaarheid en distributie van vertrouwen. Als we één van deze drie aspecten verbeteren, gaat dit ten koste van minstens één van de andere aspecten. Het is bijzonder moeilijk, misschien zelfs onmogelijk, om tot een technologische oplossing te komen die op de drie punten tegelijk sterk scoort. Eigenlijk is dit niet onlogisch. Men kan niet alle participanten in een groot, druk netwerk de verantwoordelijkheid geven om constant alles te valideren. Dit hoeft geenszins te betekenen dat blockchaintechnologie onbruikbaar is, maar wel dat ze fundamentele beperkingen heeft.

Samengevat, is blockchain een technologie die belooft de afhankelijkheid van intermediaire partijen drastisch te reduceren, maar die vandaag nog in zijn kinderschoenen staat. Het valt dus nog af te wachten in welke mate de verwachtingen daadwerkelijk zullen worden waargemaakt.